MISMO Remote Online Notarization Standards

FINAL Candidate Recommendation (CR) Version

Version 1

August 28, 2019

Standards for Remote Online Notarization

Summary

This document outlines technical and procedural guidance and establishes underlying principles that should be considered as organizations move towards implementation of Remote Online Notarization.

The intended audience includes but is not limited to: state regulators, commissioning or licensing officials; financial institutions; service providers; technology providers; title insurance underwriters; trade associations; mortgage and title/settlement service providers.

It is worth noting that these are the minimum set of technical and procedural standards and parties are free to implement additional requirements, practices or processes for the items addressed by these standards[1]. While not specifically addressed in these standards, remote online notarization system implementations should accommodate ADA (Americans with Disabilities Act) computer user interface standards and/or best practices as required by state and/or federal law[2].

Capitalized terms not defined in the text are defined in Section 7, entitled "DEFINITIONS".

1. **CREDENTIAL ANALYSIS AND AUTHENTICATION**
   The following authentication and analysis protocols are intended to support the notary public (Notary) in making the determination that satisfactory evidence of each Principal's identity has been established for a Remote Online Notarization. This section specifies standards for States to reference when identity proofing involving Knowledge-Based Authentication (KBA) and/or credential analysis is required to perform Remote Online Notarization[3]. If a State specifies additional or alternative means for identify verification aside from identify proofing or credential analysis (such as by oath or affirmation of a credible witness, by a Notary's personal knowledge of the Principal, or by other methods), such additional or alternative means are not addressed by these standards.
   a. Principal identity verification for Remote Online Notarization services must include consistent Multi-Factor Authentication procedures:
      i. Each Principal's identity credential must be verified against trusted third-party data sources;

---

[1] Mortgage lenders, insurance underwriters or other parties may impose more restrictive or additional standards based on jurisdiction, transaction type, financial implications or other factors.
[2] ADA requirements are a separate and distinct body of work and are not addressed by these standards.
[3] As of the time of this writing, KBA, and credential analysis procedures and technology are widely accepted as identity proofing processes and are therefore specifically addressed, however, MISMO supports efforts to explore and permit other types of analysis and authentication.

ii. Each Principal's identity must be bound to each individual Principal following successful Knowledge-Based Authentication, or another form of authentication or trusted third-party identity verification such as online banking authentication; and

iii. Procedures must provide for human visual comparison between the Principal's identity credential presented to the Notary and the Principal himself or herself.

b. **Credential Analysis of Government Issued Identification**

Remote Online Notarization service providers must use automated software processes to aid the Notary with their role in verifying each Principal's identity.

i. The credential must pass an authenticity test, consistent with sound commercial practices that:
   1. Use appropriate technologies to confirm the integrity of visual, physical or cryptographic security features;
   2. Use appropriate technologies to confirm that the credential is not fraudulent or inappropriately modified;
   3. Use information held or published by the issuing source or authoritative source(s), as available, to confirm the validity of credential details; and
   4. Provide the output of the authenticity test to the Notary.[4]

ii. The credential analysis procedure must enable the Notary to visually compare both of the following for consistency:
   1. The information and photo on the presented credential image; and
   2. The Principal as viewed by the Notary in real time through the audio/video system.

iii. Credential Type Requirements
   1. Must be a government-issued document meeting the requirements of the State that contains a photograph of the individual, may be imaged, photographed and video recorded under applicable state and federal law[5], and can be subjected to credential analysis.

iv. Credential Image Capture
   1. The credential image capture procedure must confirm that:
      a. The Principal is in possession of the credential at the time of the Notarial Act;
      b. Credential images submitted for credential analysis have not been manipulated; and
      c. Credential images match the credential in the Principal's possession.

[4] The output may simply indicate a "pass" or "fail" type score, or may provide more information to indicate the outcome of the authenticity test to the Notary.

[5] State or federal law may prohibit the capture of certain credential images.

2. The following general principles should be considered in the context of image resolution:
    a. Captured image resolution should be sufficient enough for the service provider to perform credential analysis per the requirements above.
    b. Image resolution should be sufficient to enable visual inspection by the Notary, including legible text and clarity of photographs, barcodes, and other credential features.
    c. All images necessary to perform visual inspection and credential analysis must be captured — e.g. U.S. Passport requires identity page; state driver's licenses require front and back.

c. **Dynamic Knowledge-Based Authentication**

Dynamic Knowledge-Based Authentication (KBA) is an identity assessment that is based on a set of questions formulated from public or private data sources. A Dynamic Knowledge-Based Authentication procedure must meet the following requirements:

i. Each Principal must answer questions and achieve a passing score.
    1. MISMO Recommends:
        a. Five questions, drawn from public or private data sources.
        b. A minimum of five possible answer choices per question.
        c. At least four of the five questions answered correctly (a passing score of 80%).
        d. All five questions answered within two minutes.

ii. Each Principal to be provided a reasonable number of attempts per Signing Session.
    1. MISMO Recommends:
        a. If a Principal fails their first quiz, they may attempt up to two additional quizzes within 48 hours from the first failure[6].
        b. During any quiz retake, a minimum of 40% (two) of the prior questions must be replaced[7].

iii. The Remote Online Notarization system provider must not include the KBA procedure as part of the video recording or as part of the system provided person-to-person video interaction between the Notary and the Signatory, and must not store the data or information presented in the KBA

[6] The standard of three total attempts within 48 hours accommodates a security provision (a maximum number of attempts per Signing Session) and a business provision (a reasonable time frame for such attempts) for a wide range of notarial scenarios. These standards also accommodate known technical limitations imposed by KBA service providers.

[7] The purpose of replacing questions in subsequent KBA quizzes is to reduce the statistical probability of an individual guessing correct answers.

questions and answers. However, the output of the KBA assessment procedure must be provided to the Notary.[8]

d. **Biometrics and Other Requirements**
Biometric sensing technologies have potential application to Remote Online Notarization in the areas of authentication, credential analysis, and identity verification. These technologies include but are not limited to: facial, voice, and fingerprint recognition.[9]

e. **Workflow Continuity Requirement**
If a Principal must exit the workflow, they must meet the criteria outlined in this section and restart the Credential Analysis and Authentication workflow from the beginning.[10]

2. AUDIO/VIDEO QUALITY

a. A reliable Remote Online Notarization operating model should consist of continuous, synchronous audio and video feeds with good clarity such that all participants can be clearly seen and understood at all times.

b. Inherent in online audio/video technology is the presence of temporary surges or spikes in quantitative measures like bitrate and/or frequency of communications and no simple technical limits are practical or prudent. Rather, a sounder approach to ensuring reliable real-time communications is to rely on the judgement of the Notary to determine the adequacy of the communications and provide direction to terminate the session if those conditions are not met[11].

c. The audio/video recording must include the person-to-person interaction required as part of the Notarial Act as defined by the State[12], must be logically associated to the electronic Audit Trail[13], and must be capable of being viewed and heard using broadly available audio/video players.

d. The video recording of the transaction documents executed in the Remote Online Notarization process is not required as part of these standards.[14]

---

[8] The output may simply indicate a "pass" or "fail" type score, and/or may provide more information to indicate the outcome of the KBA assessment to the Notary.

[9] MISMO does not offer specific guidance in applying this type of authentication protocol due to the lack of available industry standards regarding biometric technology.

[10] Principals may have to exit the workflow for various valid or invalid reasons and may do so for an unpredictable amount of time. Therefore, to simplify these standards and provide unambiguous guidance, MISMO requires a new Remote Online Notarization workflow be started each time a Principal exits the workflow.

[11] Uniform standards that take into account all potential audio/video disruptions and whether they affect the integrity of the Notarial Act are not practical, and therefore, these standards provide for human judgement to determine adequate audio/video quality.

[12] The specific activities required in the Notarial Act may vary by state and therefore are not defined here.

[13] One must be able to match the application of eSignatures, and other trackable events recorded in the Audit Trail, to the people and actions in the audio/video recording.

[14] Many documents that may be notarized in this manner may contain non-public personal information (NPI) as defined under applicable law. Therefore, MISMO does not require video capture of documents or credentials as part

3. STORAGE OF NOTARIAL RECORDS

a. Where applicable, and in accordance with State laws, rules and regulations, the Notary must maintain accurate and reliable Notarial Records. These State laws, rules and regulations may or may not require that a copy of the audio/video recording be part of a notarial journal (which may be subject to public access under State law)[15]. Notaries must have the ability to electronically capture the required Notarial Records or to direct a third party to do so on their behalf. In either case, the Remote Online Notarization system must:
   i. Facilitate the process of collecting the required Notarial Records;
   ii. Provide a method by which a Notary can access and/or export the Notarial Records; and
   iii. Provide automated backup of the Notarial Records and audio/video recording to ensure redundancy.

b. The Remote Online Notarization technology solution must employ data protection safeguards consistent with generally accepted information security standards.

c. Retention of the audio/video recording and Notarial Records by either the Notary public or their designated third party, as directed by the Notary, must adhere to the laws, directives, rules and regulations of the State.

4. POST-EXECUTION RECORDS

a. Significant actions completed as part of a Remote Online Notarization Signing Session should be recorded in an Audit Trail. Each entry in this Audit Trail should clearly indicate the action performed (e.g. addition of an electronic signature), the date/time of its performance (e.g. Coordinated Universal Time, 2018-08-21 01:14:22 UTC), the name of the party performing the action (e.g. John Doe) and the IP address of the party performing the action. Further detailed guidance on the contents of the Audit Trail or its form is beyond the scope of these standards.

b. Each document completed as part of a Remote Online Notarization should be electronically signed and rendered Tamper-Evident.

5. SECURITY CONSIDERATIONS

Remote Online Notarization technology providers must have comprehensive security programs in place to ensure privacy and data security. Technology providers should be vigilant to ensure consumer data, privacy and information security laws and regulations are satisfied through their information security programs. There are many industry accepted models, standards and frameworks for how to develop such programs.

---

of these standards. Including the documents and/or credentials in the video recording may be considered as a matter of policy on a state-by-state basis.

[15] Treatment of the audio/video recording in the context of the Notarial Record or journal is a matter of public policy and not addressed in these standards.

6. COUNTY RECORDING CONSIDERATIONS FOR ELECTRONICALLY NOTARIZED DOCUMENTS

a. The Remote Online Notarization system, process, and procedures must be capable of generating a printable version of all documents executed in the system, including but not limited to the documents executed in the Notarial Act, and associated certifications as required by the State, county and/or other governing or regulatory body.[16]

b. Any document notarized remotely online must clearly state, in the remote online notarial certificate, that the person making the acknowledgment, oath or affirmation and signing the document appeared remotely online using audio/video communication technology.

7. DEFINITIONS

a. **"Audit Trail"** means a chronological and detailed list of critical events and actions, from the beginning to the end of the Remote Online Notarization process, including the dates and times the events and actions took place and identification of the individuals and/or systems that performed the events or actions. Also known as: Audit Log or Event Log.

b. **"Knowledge-Based Authentication" or "KBA"** means an identity verification method based on knowledge of private information associated with the claimed identity of a person.[17]

c. **"Multi-Factor Authentication" or "MFA"** means a method of access control in which a user is granted access after successfully presenting identity evidence through a minimum of two of the following mechanisms: something they *have* (e.g. an ID credential), something they *know* (e.g. KBA), something they *are* (e.g. iris, retinal, thumbprint scans, facial recognition and other forms of biometric identification).

d. **"Notarial Act"** means an act, whether performed with respect to a tangible or electronic record, that a notarial officer may perform under the law of a specific State. The term includes taking an acknowledgment, administering an oath or affirmation, taking a verification on oath or affirmation, witnessing or attesting a signature, certifying or attesting a copy, and noting a protest of a negotiable instrument.[18]

e. **"Notarial Records"** means details of the Notarial Act common to the State's notarial journal or register requirements.

---

[16] While outside the scope of these standards, the concept of "papering out" and printing eNotarized documents for use in a paper county recording process may be permissible under the law of some states. These standards require electronically created documents be printable for this purpose.

[17] DIGITAL IDENTITY GUIDELINES NIST SP 800-63-3 (page 46 for definition of KBV a.k.a. KBA)

[18] Mortgage Bankers Association – American Land Title Association Model Legislation for Remote Online Notarization Sec.1 Definitions (9) "Notarial Act" page 3

f. **"Principal"** means an individual whose electronic signature is notarized in a remote online notarization; or making an oath or affirmation or an acknowledgment other than in the capacity of a witness for the remote online notarization.[19]

g. **"Record"** means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.[20]

h. **"Remote Online Notarization"** means a Notarial Act performed by means of an electronic device or process that allows a notary public and a Principal, who is not in the same physical location as the notary public, to complete a Notarial Act and communicate with each other simultaneously by sight and sound.[21]

i. **"Signing Session"** means one or more Notarial Acts performed on a single set of documents as a single event by a single Notary with one or more Principals and any applicable witnesses.

j. **"State"** means the state or jurisdiction under which the notary public is commissioned and for which the notary public is performing the Remote Online Notarization.[22]

k. **"Tamper-Evident"** A technology based process that indicates whether a change has been made to the record since the technology was applied.

---

[19] Mortgage Bankers Association – American Land Title Association Model Legislation for Remote Online Notarization Sec.1 Definitions (11) "Notarial Act" page 3

[20] RULONA Section 2. Definition for Record (Page 5)

[21] Adapted from the Mortgage Bankers Association – American Land Title Association Model Legislation for Remote Online Notarization Sec.1 Definitions (13) "Remote online notarization" page 4 and "(2) "Communication technology" page 1.

[22] This state definition provides clarity for which jurisdiction rules, requirements or regulations must be referenced when there is more than one state related to a Notarial Act: (1) the state where the Principal is located, (2) the state where a property related to the Notarial Act is located, (3) the state in which the Notary is located, or (4) other state references.